BLE安全研究的基础设施建设

李海粟（BACKAHASTEN）

通信安全研究我们需要什么？

- 无障碍接收数据包
- 无障碍发射数据包

BLE特性

- 跳频 ---------最大困难
- 进入数据信道后，所有的常规信息全部消失 ------信息恢复
- 基带封闭 ----------使用GNU Radio

GNU RADIO的一些小窍门（流图，代码讲解）

- GFSK Demod
- 动态参数
- 异步消息
- 外部流图调用

BLE跳频规则（P 2206）

LLData									
AA (4 octets)	CRCInit (3 octets)	WinSize (1 octet)	WinOffset (2 octets)	Interval (2 octets)	Latency (2 octets)	Timeout (2 octets)	ChM (5 octets)	Hop (5 bits)	SCA (3 bits)

Figure 2.11: LLData field structure in CONNECT_REQ PDU's payload

- AA --目标地址
- CRCINIT --校验初始化
- WINSIZE --窗口大小
- WINOFFSET --使用时间段
- INTERVAL --频道时长
- LATENCY --连接数
- TIMEOUT --超时
- CHM --信道质量
- HOP --跳频参数
- SCA --时钟精度

信息恢复的一般思路（流图代码讲解）

- 通过前导码初步获取一个包的位置
- 使用RUF过滤
- 使用两次Access address确定access address
- 使用PDU和CRC恢复出CRCinit

信道信息恢复（约束性编程讲解，代码讲解）

- CRCinit
- Access address
- Hop（todo）

信道信息恢复（广播开启）

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
4	+555020	0x26	0x8E89BED6	ADV_DISCOVER_IND	Type TxAdd RxAdd PDU-Length 6 1 0 37	0xEF29EEC7F967	02 01 04 1B FF 57 01 00 B1 3B AD EC 39 BF BB B7	0xD8FB1C	-48	OK
5	+550020	0x26	0x8E89BED6	ADV_DISCOVER_IND	Type TxAdd RxAdd PDU-Length 6 1 0 37	0xEF29EEC7F967	02 01 04 1B FF 57 01 00 B1 3B AD EC 39 BF BB B7	0xD8FB1C	-47	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	ScanA	AdvA	CRC	RSSI (dBm)	FCS
6	+526	0x26	0x8E89BED6	ADV_SCAN_REQ	Type TxAdd RxAdd PDU-Length 3 1 1 12	0x6902FA3468D8	0xEF29EEC7F967	0xF70AE2	-29	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	ScanRspData	CRC	RSSI (dBm)	FCS
7	+325	0x26	0x8E89BED6	ADV_SCAN_RSP	Type TxAdd RxAdd PDU-Length 4 1 0 29	0xEF29EEC7F967	0A 09 4D 49 20 42 61 6E 64 20 32 03	0x8B82EF	-47	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
8	+547919	0x26	0x8E89BED6	ADV_DISCOVER_IND	Type TxAdd RxAdd PDU-Length 6 1 0 37	0xEF29EEC7F967	02 01 04 1B FF 57 01 00 B1 3B AD EC 39 BF BB B7	0xD8FB1C	-48	OK
9	+546272	0x26	0x8E89BED6	ADV_DISCOVER_IND	Type TxAdd RxAdd PDU-Length 6 1 0 37	0xEF29EEC7F967	02 01 04 1B FF 57 01 00 B1 3B AD EC 39 BF BB B7	0xD8FB1C	-49	OK

实习成果：

① GNURADIO OOT模块

② 发表文章，复杂GNU RADIO OOT模块的设计(DOING)

③ 发表文章，如何嗅探数据信道的BLE数据包(DOING)

TODO

- 完美跟踪一个设备的跳频（蓝牙中继攻击）
- 蓝牙自组网安全性研究

未来

- Mesh（协议于7月13日颁布）
- 蓝牙5.0（芯片开始大规模出货）